PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-322353
(43)Date of publication of application : 24.11.2000

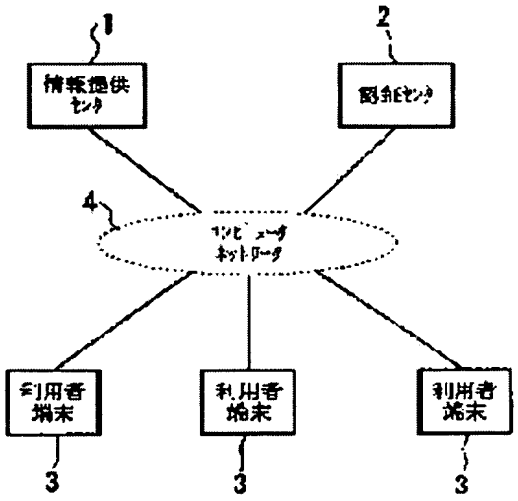
(51)Int.Cl. G06F 13/00
G06F 15/00
G06F 17/60

(21)Application number : 11-133298
(22)Date of filing : 13.05.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : TAKEUCHI ITARU
SUZUKI HIDEAKI
SONEOKA AKINAO

(54) INFORMATION PROVIDING DEVICE, INFORMATION PROVIDING SERVICE AUTHENTICATING METHOD AND RECORDING MEDIUM FOR RECORDING INFORMATION PROVIDING SERVICE AUTHENTICATION PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information providing device simplified in authentication processing to be operated by a user while holding the function of the authentica tion processing.
SOLUTION: An information providing center 1 is provided with an information contents database which records information to be provided to user's terminals 3, a service pass table which records a service pass for applying authority to receive a service to the user's terminals 3, and an information providing part which issues the service pass recorded in the service pass table based on a result obtained by inspecting authentication information inputted from the user's terminals 3, and which provides the information recorded in the information contents database to the user's terminals 3. The user's terminal 3 is provided with an information display part which displays the information provided by the information providing center 1 and a service pass holder which records the service pass provided by the information providing center 1.



LEGAL STATUS

[Date of request for examination] 13.08.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Citation B

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－322353
（Ｐ２０００－３２２３５３Ａ）
(43)公開日　平成12年11月24日(2000.11.24)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ			テーマコード（参考）
G06F 13/00	351	G06F 13/00	351	Z	5B049
15/00	310	15/00	310	A	5B085
	330		330	A	5B089
17/60		15/21	340	B	

審査請求　未請求　請求項の数10　ＯＬ　（全10頁）

(21)出願番号　特願平11－133298

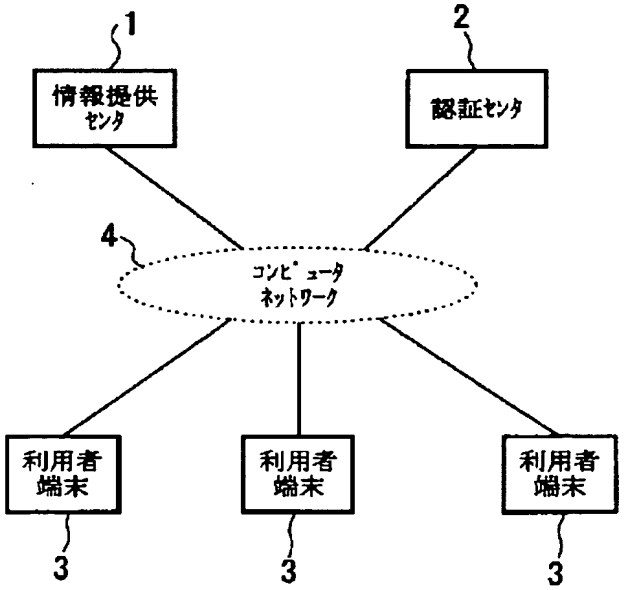
(22)出願日　平成11年５月13日(1999.5.13)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　竹内　格
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　鈴木　英明
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100064908
弁理士　志賀　正武

最終頁に続く

(54)【発明の名称】情報提供装置、情報提供サービス認証方法及び情報提供サービス認証プログラムを記録した記録媒体

(57)【要約】
【課題】　認証処理の機能を保ちつつ利用者が行う認証処理を簡略化することができる情報提供装置を提供することを目的とする。
【解決手段】　情報提供センタは、利用者端末に対して提供する情報が記録された情報コンテンツ・データベースと、利用者端末に対してサービスを受ける権利を与えるサービスパスを記録するサービスパス・テーブルと、利用者端末から入力された認証情報を認証センタが検査した結果に基づいてサービスパス・テーブルに記録されたサービスパスの発行と情報コンテンツ・データベースに記録された情報を利用者端末に対して提供する情報提供部とを備え、利用者端末は、情報提供センタから提供された情報を表示する情報表示部と、情報提供センタから提供されたサービスパスを記録するサービスパス・ホルダとを備えたことを特徴とする。



1

【特許請求の範囲】

【請求項１】　情報を利用者に対して提供する情報提供センタと、利用者が正当な利用者か否かを検査する認証センタと、情報の提供を受ける利用者端末とを備えた情報提供サービスを行う情報提供装置において、

前記情報提供センタは、

前記利用者端末に対して提供する情報が記録された情報コンテンツ・データベースと、

前記利用者端末に対してサービスを受ける権利を与えるサービスパスを記録するサービスパス・テーブルと、

前記利用者端末から入力された認証情報を認証センタが検査した結果に基づいて前記サービスパス・テーブルに記録されたサービスパスの発行と前記情報コンテンツ・データベースに記録された情報を前記利用者端末に対して提供する情報提供部と、

を備えたことを特徴とする情報提供センタ。

【請求項２】　情報を利用者に対して提供する情報提供センタと、利用者が正当な利用者か否かを検査する認証センタと、情報の提供を受ける利用者端末とを備えた情報提供サービスを行う情報提供装置において、

前記利用者端末は、

前記情報提供センタから提供された情報を表示する情報表示部と、

前記情報提供センタから提供されたサービスパスを記録するサービスパス・ホルダと、

を備えたことを特徴とする利用者端末。

【請求項３】　情報を利用者に対して提供する情報提供センタと、利用者が正当な利用者か否かを検査する認証センタと、情報の提供を受ける利用者端末とを備えた情報提供サービスを行う情報提供装置における情報提供サービス認証方法であって、

前記情報提供サービス認証方法は、

利用者がサービスを受ける際に、認証センタが利用者端末から入力された認証情報の正当性を検査する処理と、

認証情報の正当性が確認された場合に、情報提供センタが利用者端末に対して情報提供をするとともにサービスパスを発行する処理と、

発行された前記サービスパスを利用者端末内に記録する処理と、

を有することを特徴とする情報提供サービス認証方法。

【請求項４】　前記情報提供サービス認証方法は、

利用者がサービスを受ける際に、サービスパスが既に記録されている場合に記録されているサービスパスを情報提供センタに対して提示する処理と、

提示されたサービスパスの正当性を検査する処理と、

前記正当性の検査結果に基づいて、情報提供を行う処理と、

をさらに有することを特徴とする請求項３に記載の情報提供サービス認証方法。

【請求項５】　前記情報提供サービス認証方法は、

2

提示されたサービスパスの正当性を検査し、このサービスパスの正当性が確認された場合にすでに発行したサービスパスとは異なる新しいサービスパスを利用者端末に対して発行する処理をさらに有することを特徴とする請求項４に記載の情報提供サービス認証方法。

【請求項６】　前記情報提供サービス認証方法は、

不正なサービスパスが提示された場合に再度認証情報の入力を要求する処理と、

入力された認証情報の正当性を検査して、その正当性が確認された場合に新たなサービスパスを発行する処理と、

をさらに有することを特徴とする請求項４または５に記載の情報提供サービス認証方法。

【請求項７】　情報を利用者に対して提供する情報提供センタと、利用者が正当な利用者か否かを検査する認証センタと、情報の提供を受ける利用者端末とを備えた情報提供サービスを行う情報提供装置における情報提供サービス認証プログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記情報提供サービス認証プログラムは、

利用者がサービスを受ける際に、認証センタが利用者端末から入力された認証情報の正当性を検査する処理と、

認証情報の正当性が確認された場合に、情報提供センタが利用者端末に対して情報提供をするとともにサービスパスを発行する処理と、

発行された前記サービスパスを利用者端末内に記録する処理と、

をコンピュータに行わせることを特徴とする情報提供サービス認証プログラムを記録した記録媒体。

【請求項８】　前記情報提供サービス認証プログラムは、

利用者がサービスを受ける際に、サービスパスが既に記録されている場合に記録されているサービスパスを情報提供センタに対して提示する処理と、

提示されたサービスパスの正当性を検査する処理と、

前記正当性の検査結果に基づいて、情報提供を行う処理と、

をさらにコンピュータに行わせることを特徴とする請求項７に記載の情報提供サービス認証プログラムを記録した記録媒体。

【請求項９】　前記情報提供サービス認証プログラムは、

提示されたサービスパスの正当性を検査し、このサービスパスの正当性が確認された場合にすでに発行したサービスパスとは異なる新しいサービスパスを利用者端末に対して発行する処理をさらにコンピュータに行わせることを特徴とする請求項８に記載の情報提供サービス認証プログラムを記録した記録媒体。

【請求項１０】　前記情報提供サービス認証プログラムは、

不正なサービスパスが提示された場合に再度認証情報の入力を要求する処理と、
入力された認証情報の正当性を検査して、その正当性が確認された場合に新たなサービスパスを発行する処理と、
をさらにコンピュータに行わせることを特徴とする請求項８または９に記載の情報提供サービス認証プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータネットワークを介して、有料のオンラインニュースなどを、特定のユーザ群へ情報サービスを提供する際の利用者を認証する情報提供装置、情報提供サービス認証方法及び情報提供サービス認証プログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】コンピュータネットワークを介して有料オンラインニュースなどの情報サービスを提供する際に利用者を認証するには、情報提供センタが各利用者に用意するアカウントの認証情報（例えば、利用者ＩＤとパスワードなど）を入力させることにより対処してきた。

【０００３】

【発明が解決しようとする課題】しかしながら、従来の方法では、利用者は情報提供サービスを受けようとする度に、認証情報を入力する必要があり、利用者にとっては手間がかかり、これは非常に煩わしいという問題がある。

【０００４】本発明は、このような事情に鑑みてなされたもので、認証処理の機能を保ちつつ利用者が行う認証処理を簡略化することができる情報提供装置、情報提供サービス認証方法及び情報提供サービス認証プログラムを記録した記録媒体を提供することを目的とする。

【０００５】

【課題を解決するための手段】請求項１に記載の発明は、情報を利用者に対して提供する情報提供センタと、利用者が正当な利用者か否かを検査する認証センタと、情報の提供を受ける利用者端末とを備えた情報提供サービスを行う情報提供装置において、前記情報提供センタは、前記利用者端末に対して提供する情報が記録された情報コンテンツ・データベースと、前記利用者端末に対してサービスを受ける権利を与えるサービスパスを記録するサービスパス・テーブルと、前記利用者端末から入力された認証情報を認証センタが検査した結果に基づいて前記サービスパス・テーブルに記録されたサービスパスの発行と前記情報コンテンツ・データベースに記録された情報を前記利用者端末に対して提供する情報提供部とを備えたことを特徴とする。

【０００６】請求項２に記載の発明は、情報を利用者に対して提供する情報提供センタと、利用者が正当な利用者か否かを検査する認証センタと、情報の提供を受ける利用者端末とを備えた情報提供サービスを行う情報提供装置において、前記利用者端末は、前記情報提供センタから提供された情報を表示する情報表示部と、前記情報提供センタから提供されたサービスパスを記録するサービスパス・ホルダとを備えたことを特徴とする。

【０００７】請求項３に記載の発明は、情報を利用者に対して提供する情報提供センタと、利用者が正当な利用者か否かを検査する認証センタと、情報の提供を受ける利用者端末とを備えた情報提供サービスを行う情報提供装置における情報提供サービス認証方法であって、前記情報提供サービス認証方法は、利用者がサービスを受ける際に、認証センタが利用者端末から入力された認証情報の正当性を検査する処理と、認証情報の正当性が確認された場合に、情報提供センタが利用者端末に対して情報提供をするとともにサービスパスを発行する処理と、発行された前記サービスパスを利用者端末内に記録する処理とを有することを特徴とする。

【０００８】請求項４に記載の発明は、前記情報提供サービス認証方法は、利用者がサービスを受ける際に、サービスパスが既に記録されている場合に記録されているサービスパスを情報提供センタに対して提示する処理と、提示されたサービスパスの正当性を検査する処理と、前記正当性の検査結果に基づいて、情報提供を行う処理とをさらに有することを特徴とする。

【０００９】請求項５に記載の発明は、前記情報提供サービス認証方法は、提示されたサービスパスの正当性を検査し、このサービスパスの正当性が確認された場合にすでに発行したサービスパスとは異なる新しいサービスパスを利用者端末に対して発行する処理をさらに有することを特徴とする。

【００１０】請求項６に記載の発明は、前記情報提供サービス認証方法は、不正なサービスパスが提示された場合に再度認証情報の入力を要求する処理と、入力された認証情報の正当性を検査して、その正当性が確認された場合に新たなサービスパスを発行する処理とをさらに有することを特徴とする。

【００１１】請求項７に記載の発明は、情報を利用者に対して提供する情報提供センタと、利用者が正当な利用者か否かを検査する認証センタと、情報の提供を受ける利用者端末とを備えた情報提供サービスを行う情報提供装置における情報提供サービス認証プログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記情報提供サービス認証プログラムは、利用者がサービスを受ける際に、認証センタが利用者端末から入力された認証情報の正当性を検査する処理と、認証情報の正当性が確認された場合に、情報提供センタが利用者端末に対して情報提供をするとともにサービスパスを発行する処理と、発行された前記サービスパスを利用者端末内に記録する処理とをコンピュータに行わせることを特徴とす

る。

【００１２】請求項８に記載の発明は、前記情報提供サービス認証プログラムは、利用者がサービスを受ける際に、サービスパスが既に記録されている場合に記録されているサービスパスを情報提供センタに対して提示する処理と、提示されたサービスパスの正当性を検査する処理と、前記正当性の検査結果に基づいて、情報提供を行う処理とをさらにコンピュータに行わせることを特徴とする。

【００１３】請求項９に記載の発明は、前記情報提供サービス認証プログラムは、提示されたサービスパスの正当性を検査し、このサービスパスの正当性が確認された場合にすでに発行したサービスパスとは異なる新しいサービスパスを利用者端末に対して発行する処理をさらにコンピュータに行わせることを特徴とする。

【００１４】請求項１０に記載の発明は、前記情報提供サービス認証プログラムは、不正なサービスパスが提示された場合に再度認証情報の入力を要求する処理と、入力された認証情報の正当性を検査して、その正当性が確認された場合に新たなサービスパスを発行する処理とをさらにコンピュータに行わせることを特徴とする。

【００１５】

【発明の実施の形態】以下、本発明による情報提供装置、情報提供サービス認証方法及び情報提供サービス認証プログラムを記録した記録媒体を図面を参照して説明する。図１は情報提供装置の全体構成を示すブロック図である。この図において、符号１は、情報提供を受ける権利を持つ各利用者に対して情報提供を行なう情報提供センタである。符号２は、利用者の認証を行なう認証センタである。符号３は、情報提供センタ１、認証センタ２に接続することによってサービスを受ける利用者端末である。符号４は、情報提供センタ１、認証センタ２、利用者端末３をそれぞれ接続するコンピュータネットワークであり、インターネットであってもよい。

【００１６】＜第１の実施形態＞図２は、図１に示す情報提供センタ１および利用者端末３の構成を示す図である。情報提供センタ１は、利用者に対して情報提供を行なう情報提供部１１と、利用者に発行したサービスパスを記録するサービスパステーブル１２と、利用者に提供する情報の情報コンテンツ・データベース１３とからなる。利用者端末３は、情報表示部３１と情報表示部３１が情報提供部１１から受け取ったサービスパスを保存するサービスパス・ホルダ３２とからなる。

【００１７】ここでいうサービスパスとは、情報提供センタ１から情報提供サービスを受ける権利に相当するものであり、このサービスパスを持つ利用者だけが、情報提供センタから情報提供サービスを受けることができる。また、サービスパスは、利用者の「ユーザＩＤ」、「タイムスタンプ」及び利用者端末３の「端末情報」からなるデータである。「ユーザＩＤ」とは、利用者端末３の所有者を識別するためのコードであり、情報提供センタ１において一意となるユーザＩＤが予め登録されている。「タイムスタンプ」とは、サービスパス発行時の日時をコード化したものであり、サービスパス発行毎に異なるコードとなる。「端末情報」とは、情報提供センタ１に接続される利用者端末３を識別するためのコードであり、この利用者端末３に割り当てられたＩＰアドレス等が用いられる。

【００１８】次に、図２、５を参照して、利用者がサービスパスを取得する動作を説明する。図５は、利用者がサービスパスを取得する動作を示すシーケンス図である。以下の説明において、情報提供センタ１、認証センタ２及び複数の利用者端末３はそれぞれコンピュータネットワーク４に接続されているが、特に説明がない場合は、このコンピュータネットワーク４を介してデータ等の送受が行われるものとする。

【００１９】まず、利用者は利用者端末３を用い、認証センタ２に対して認証情報を送る。ここでいう認証情報とは、利用者ＩＤとパスワード等であり、利用者の認証を行なうのに一般的に必要な情報を指す。認証センタ２は、受け取ったこの認証情報をチェックして、その認証結果を情報提供部１１へ送信する。このとき、認証センタ２は、受け取った認証情報が正しいものであるなら、情報提供センタ１に対してサービスパス発行通知を出し、正しくないものであった場合は、その旨を通知する。

【００２０】次に情報提供部１１は、認証センタ２から受け取った認証結果に基づいて、認証情報が正しいものであった場合は新規のサービスパスを生成し、それをサービスパス・テーブル１２に記録するとともに利用者端末３の情報表示部３１へ送信する。これを受けて、利用者端末３の情報表示部３１は、情報提供部１１から受け取ったサービスパスをサービスパス・ホルダ３２に記録する。

【００２１】なお、サービスパスの内容としては、その利用者の「ユーザＩＤ」、発行時の「タイムスタンプ」、そして利用者の「端末情報」などが使われる。これらを組み合わせた文字列から既存の暗号化やハッシュ関数などを使って変換して得られる値を用いることによって、その内容が利用者から簡単に想像不可能であり、かつ毎回異なる値とすることができるため、サービスパスとして使用することができる。また、情報提供部１１と認証センタ２との通信、および、利用者端末３と認証センタ２との通信には、第三者が介入できないような秘密通信が使用できるようなネットワーク環境となっているものとする。さらに、サービスパスには、予め定められた有効期限が設定されており、この有効期限を過ぎたサービスパスは、正規の利用者であっても使用できなくなる。

【００２２】次に、図６を参照して、利用者が情報提供

を受ける動作を説明する。図６は、利用者が情報提供を受ける動作を示すシーケンス図である。まず、利用者端末３の情報表示部３１はサービスパス・ホルダ３２からサービスパスを取りだし、情報提供センタ１の情報提供部１１に対して、情報コンテンツ要求とサービスパスを送る。ここでいう情報コンテンツ要求とは、情報コンテンツの名前や識別子等であり、例えばＷｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ（以下、WWWと称する）で言えば、ＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）のような情報コンテンツを特定するものとする。

【００２３】情報提供部１１では、情報提供部から渡されたサービスパスが自身が発行したものであるか否かをサービスパス・テーブル１２を参照することによって、サービスパスのチェックを行う。その結果、正しいものであれば、サービスパス・テーブル１２において、そのサービスパスを無効化し、代わりに新規のサービスパスを生成してサービスパス・テーブル１２を更新する。

【００２４】そして、情報表示部３１からの情報コンテンツ要求に対応するものを、情報コンテンツ・データベース１３を検索することによって取得し、その情報コンテンツと新規に生成したサービスパスとを情報表示部３１に対して送信する。情報表示部３１は、サービスパス・ホルダ３２に記録されているサービスパスを、この受け取ったサービスパスとの入れ替えることによって、サービスパス・ホルダ３２の内容を更新し、情報コンテンツは図示しないディスプレイ等に表示する。

【００２５】このように、情報提供を受ける際に毎回認証情報を入力するかわりに、サービスパスを取得してこのサービスパスを利用することにより、一度認証情報を入力すれば以降は認証情報の入力なしに情報サービスをうけることが可能となる。

【００２６】次に、図７を参照して、不正なサービスパスが情報提供センタ１に提示された場合について説明する。まず、利用者は情報表示部３１を使い、情報コンテンツ要求とサービスパスを情報提供センタ１へ送る。ここで送信されたサービスパスは不正なサービスパスであるものとする。情報提供センタ１の情報提供部１１は、受け取ったサービスパスが正しいものであるかをサービスパステーブル１２を参照することによって調べる。このとき、情報提供部１１は、受け取ったサービスパスが、自身の発行したものであるか、あるいは有効期限内であるかによって、このサービスパスが無効であるか否かを判断する。

【００２７】この判断の結果、無効となっているものであると判断すると、情報提供部１１は情報表示部３１に対して認証情報入力要求を出す。情報表示部３１は利用者端末３のディスプレイ等に認証情報入力画面を表示し、利用者は認証情報を入力する。情報表示部３１は入力された認証情報を認証センタ２に送信し、認証センタ２では受け取った認証情報の正当性を検査しそれが正しいものなら、情報提供センタ１にサービスパス発行通知を出す。

【００２８】情報提供センタ１の情報提供部１１は、新規のサービスパスを生成し、それをサービスパス・テーブル１２に記録し、はじめに利用者が提示してきた情報コンテンツ要求に対応するものを情報コンテンツ・データベース１３から取得し、その情報コンテンツと新規に生成したサービスパスとを情報表示部３１に送信する。情報表示部３１では受け取ったサービスパスはサービスパス・ホルダ３２に記録し、情報コンテンツは利用者に表示する。

【００２９】このように、利用者がサービスを受けるたびに毎回サービスパスが更新されるため、サービスパスが不正な第三者に盗まれ一度でもそれを使って第三者がサービスを受けてしまうと、正規の利用者の持っているサービスパスが無効となってしまうため、正規の利用者はサービスを受けられなくなる。しかし、サービス提供側から見れば、同時にサービスを受ける利用者の数は常に保たれ、サービス使用ライセンスの数を保持することができる。

【００３０】また、サービスパスが盗まれたとしても、正規の利用者は再び認証情報を入力して新規のサービスパスを取得すれば、サービスが受けられるようになり、同時に盗まれたサービスパスが無効となるため、不正利用からの復活を容易に行なうことができる。

【００３１】＜第２の実施形態＞次に、インターネットで一般的に用いられているWWWを利用した場合の実施形態について説明する。図３は、第２の実施形態の構成を示すブロック図である。図３に示す構成が図２に示す構成と異なる点は、情報提供部１１をWWWサーバ１１ａと情報提供ＣＧＩ部１１ｂによって構成されるようにしたことと、情報表示部３１及びサービスパス・ホルダ３２をそれぞれWWWブラウザ３１ａ及びクッキー・ファイル３２ａで構成した点である。

【００３２】次に、利用者がサービスパスを取得する動作を説明する。利用者がサービスパスを所有していない場合のサービスパスの取得は次のようにして行なわれる。インターネットに接続しているパーソナルコンピュータなどの利用者端末３において、利用者はWWWブラウザ３１ａを用いて、認証センタ２に対して認証情報を送る。ここでいう認証情報とは、第１の実施形態において説明したものと同等である。

【００３３】認証センタ２では、受け取った認証情報をチェックし、それが正しいか否かの認証結果を、情報提供ＣＧＩ部１１ｂに対して回答する。情報提供ＣＧＩ部１１ｂでは、認証センタ２から利用者の認証情報が正しいものであると回答を受けた場合には、新規のサービスパスを生成し、それをサービスパス・テーブル１２に記録し、利用者端末３のWWWブラウザ３１ａにクッキーデータとして送信する。利用者端末３のWWWブラウザ

３１ａは、情報提供センタ１から受け取ったサービスパスのクッキーデータをクッキーファイル３２ａに記録する。

【００３４】ここで、ＣＧＩとは、Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅの略であり、WWWサーバから他の外部プログラムを起動するインターフェースを指し、サーバから起動される外部プログラムは　ＣＧＩプログラムなどと呼ばれる。また、クッキーデータとは、一般的なブラウザとサーバ間での通信プロトコルである　ＨＴＴＰを用いてやりとりすることの可能な補助的なデータであり、通常一般的なブラウザで使用可能である。

【００３５】なお、サービスパスの内容としては、その利用者の「ユーザＩＤ」、発行時の「タイムスタンプ」、そして利用者の「端末情報」などが使われる。これらを組み合わせた文字列から既存の暗号化やハッシュ関数などを使って変換して得られる値を用いることによって、その内容が利用者から簡単に想像不可能であり、かつ毎回異なる値とすることができるため、サービスパスとして使用することができる。例えば、一方向の暗号化関数であるハッシュ関数を利用し、利用者の接続時刻あるいは乱数のような常に異なる値をハッシュ関数にかけることにより、利用者から想像不可能かつ毎回異なる文字列を生成することができ、これをサービスパスとして使用することができる。

【００３６】また、情報提供ＣＧＩ部１１ｂと認証センタ２との通信には第三者が介入できないような秘密通信が使用できるようなネットワーク環境となっているものとする。これは例えばバーチャル・プライベート・ネットワーク（ＶＰＮ）と呼ばれる第三者の介在できない秘密通信ネットワークなどを用いることにより実現することができる。

【００３７】次に、利用者が情報提供を受ける動作を説明する。まず、利用者端末３のWWWブラウザ３１ａはクッキーファイル３２ａからサービスパスを取りだし、情報提供センタ１のWWWサーバ１１ａに、情報コンテンツ要求と、サービスパスをクッキーデータとして送る。ここではWWWを前提としている為、情報コンテンツ要求とは、WWWの通信プロトコルであるＨＴＴＰに基づいたフォーマットであり、情報コンテンツの指定にはＵＲＬが使われる。

【００３８】WWWサーバ１１ａは情報提供ＣＧｌ部１１ｂを起動し、情報提供ＣＧＩ部１１ｂは渡されたサービスパスが自身の発行したものか否かをサービスパス・テーブル１２を参照してチェックする。正しいものであれば、サービスパス・テーブル１２においてそのサービスパスを無効とし、代わりに新規のサービスパスを生成してサービスパス・テーブル１２を更新する。そして、指定されたＵＲＬに対応するものを情報コンテンツ・データベース１３を検索することによって取得して、新規に生成したサービスパスからなるクッキーデータと、情報コンテンツとをＨＴＴＰプロトコルでブラウザ３１ａに対して送信する。WWWブラウザ３１ａではクッキーデータとして受け取ったサービスパスをクッキーファイル３２ａに記録し、情報コンテンツを利用者に対して表示する。

【００３９】次に、不正なサービスパスが情報提供センタ１に提示された場合の動作を説明する。まず、利用者はブラウザ３１ａを使い、情報コンテンツ要求とサービスパスからなるクッキーデータを情報提供センタ１へ送る。ここで送信されるサービスパスは不正なサービスパスであるものとする。続いて、情報提供センタ１のサーバ１１ａは情報提供ＣＧＩ部１１ｂを起動して、情報提供ＣＧＩ部１１ｂは受け取ったサービスパスが正しいものかサービスパステーブル１２で調べる。このとき、自身の発行したものでないかあるいはすでに無効となっているものであると判断すると、WWWブラウザ３１ａに対して認証情報入力要求を出す。

【００４０】WWWブラウザ３１ａは利用者端末３のディスプレイ等に認証情報入力画面を表示し、利用者は認証情報を入力する。ブラウザ３１ａは入力された認証情報を認証センタ２に送信し、認証センタ２は受け取った認証情報の正当性を検査しそれが正しいものなら、情報提供センタ１の情報提供ＣＧＩ部１１ｂにサービスパス発行通知を出す。情報提供ＣＧＩ部１１ｂは、新規のサービスパスを生成し、それをサービスパス・テーブル１２に記録し、はじめに利用者が提示してきた情報コンテンツ要求に対応するものを情報コンテンツ・データベース１３から取得し、その情報コンテンツと新規に生成したサービスパスからなるクッキーデータとをＨＴＴＰプロトコルによってブラウザ３１ａへ送信する。ブラウザ３１ａでは受け取ったサービスパスのクッキーデータをクッキー・ファイル３２ａに記録し、情報コンテンツを利用者に表示する。

【００４１】＜第３の実施形態＞次に、インターネットで一般的に用いられているWWWを利用した場合の実施形態において、WWWブラウザと認証センタとの認証情報の受け渡しに情報提供センタを中継する場合について図４を参照して説明する。図４は、第３の実施形態の構成を示すブロック図である。

【００４２】インターネットに接続されているパーソナルコンピュータなどの利用者端末３において、利用者はWWWブラウザ３１ａからＨＴＴＰプロトコルを用いて、情報提供センタ１へ認証情報を送る。ここでいう認証情報とは、第１の実施形態において説明したものと同等である。

【００４３】情報提供センタ１のWWWサーバ１１ａはWWWブラウザ３１ａからの認証情報を認証センタ２へ転送する。認証センタ２では、情報提供センタ１から受け取った認証情報をチェックし、それが正しいか不正か

の認証結果を、情報提供ＣＧＩ部１１ｂへ回答する。情報提供ＣＧＩ部１１ｂでは、認証センタ２から利用者の認証情報が正しいものであると回答を受けた場合には、新規のサービスパスを生成し、それをサービスパス・テーブル１２に記録し、利用者のWWWブラウザ３１ａにクッキーデータとして送信する。利用者端末３のWWWブラウザ３１ａでは、情報提供センタ１から受け取ったサービスパスのクッキーデータをクッキーファイル３２ａへ記録する。

【００４４】次に、利用者が情報提供を受ける動作を説明する。まず、利用者端末３のWWWブラウザ３１ａはクッキーファイル３２ａからサービスパスを取りだし、情報提供センタ１のWWWサーバ１１ａに、情報コンテンツ要求と、サービスパスをクッキーデータとして送る。ここではWWWを前提としている為、情報コンテンツ要求とは、WWWの通信プロトコルであるＨＴＴＰに基づいたフォーマットであり、情報コンテンツの指定にはＵＲＬが使われる。

【００４５】WWWサーバ１１ａは情報提供ＣＧＩ部１１ｂを起動し、情報提供ＣＧＩ部１１ｂは渡されたサービスパスが自分の発行したものかどうかをサービスパス・テーブル１２を参照してチェックする。正しいものであれば、サービスパス・テーブル１２においてそのサービスパスを無効とし、かわりに新規のサービスパスを生成してサービスパス・テーブル１２を更新し、指定されたＵＲＬに対応するものを情報コンテンツ・データベース１３から取得して、新規に生成したサービスパスからなるクッキーデータと、情報コンテンツとをＨＴＴＰプロトコルでWWWブラウザ３１ａに送信する。WWWブラウザ３１ａではクッキーデータとして受け取ったサービスパスをクッキーファイル３２ａに記録し、情報コンテンツを利用者に表示する。

【００４６】次に、不正なサービスパスが情報提供センタ１に提示された場合の動作を説明する。まず、利用者はWWWブラウザ３１ａを使い、情報コンテンツ要求と不正なサービスパスからなるクッキーデータを情報提供センタ１へ送る。情報提供センタ１のWWWサーバ１１ａは情報提供ＣＧＩ部１１ｂを起動し、情報提供ＣＧＩ部１１ｂは受け取ったサービスパスが正しいものかサービスパステーブル１２を参照して調べる。その結果、自身の発行したものでないかあるいはすでに無効となっているものであると判断すると、WWWブラウザ３１ａに対して認証情報入力要求を出す。WWWブラウザ３１ａは利用者端末のディスプレイ等に認証情報入力画面を表示し、利用者は認証情報を入力する。WWWブラウザ３１ａは入力された認証情報を情報提供センタ１へ送信し、それを情報提供センタ１のWWWサーバ１１ａは認証センタ２へ転送する。

【００４７】次に、認証センタ２では受け取った認証情報の正当性を検査しそれが正しいものなら、情報提供センタ１の情報提供ＣＧＩ部１１ｂにサービスパス発行通知を出す。情報提供ＣＧＩ部１１ｂは、新規のサービスパスを生成し、それをサービスパス・テーブル１２に記録し、はじめに利用者が提示してきた情報コンテンツ要求に対応するものを情報コンテンツ・データベース１３から取得し、その情報コンテンツと新規に生成したサービスパスからなるクッキーデータとをＨＴＴＰプロトコルでWWWブラウザ３１ａに送信する。WWWブラウザ３１ａでは受け取ったサービスパスのクッキーデータをクッキー・ファイル３２ａに記録し、情報コンテンツを利用者に表示する。

【００４８】この実施形態では、利用者端末３から認証センタ２への認証情報を受け渡すのに、情報提供センタ２が中継の役割を果たしている。この実施形態は、情報提供センタ１が認証センタ２にとって信頼のおけるものである場合であり、つまり、利用者が認証センタへ宛てた認証情報を、情報提供センタが不正に複製したり偽造するというような悪意のないものである場合にのみ実施が可能である。

【００４９】また、この実施形態の場合には情報提供サービスにおけるサービスの流れを情報提供センタ１で一元管理しやすいという利点もある。この実施形態においても、情報提供センタ１と認証センタ２の間の通信には第三者の介入できない秘密通信が使用されることが前提である。

【００５０】なお、利用者端末３の起動時において、この利用者端末３の所有者であるか否かをパスワードなどによってチェックして、他人が利用端末３を不正利用することを防止するようにしてもよい。

【００５１】また、図５、６、７に示す各処理を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより情報提供サービス認証処理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。また、「コンピュータシステム」は、WWWシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フロッピーディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

【００５２】さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの（伝送媒体ないしは伝送波）、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持している

ものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【００５３】

【発明の効果】以上説明したように、この発明によれば、利用者はサービスパスを取得して、このサービスパスが有効な期間であれば、認証情報の入力をすることなく情報サービスをうけることが可能となるため、サービス提供時において入力の手間を省くことができるという効果が得られる。

【００５４】また、この発明によれば、同時にサービスを受けることはできる利用者の数を常に一定に保つことができ、サービス使用ライセンスの数を保持することができるという効果も得られる。

【００５５】また、この発明によれば、正規の利用者は再び認証情報を入力して新規のサービスパスを取得することにより、第三者による不正利用からの復活および、盗まれたサービスパスを無効にすることを容易に行なうことができるという効果も得られる。

【図面の簡単な説明】

【図１】本発明による情報提供装置の全体構成を示すブロック図である。

【図２】本発明の第１の実施形態の構成を示すブロック図である。

【図３】本発明の第２の実施形態の構成を示すブロック図である。

【図４】本発明の第３の実施形態の構成を示すブロック図である。

【図５】サービスパスを取得する際の動作を示すシーケンス図である。

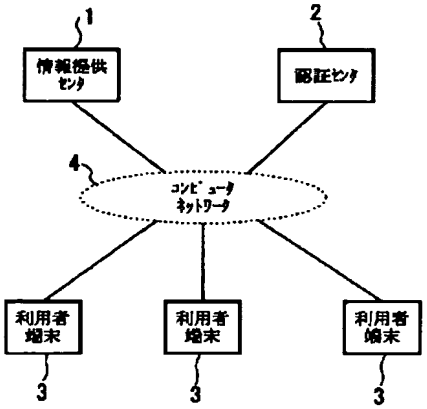
【図６】情報提供サービスを受ける動作を示すシーケンス図である。

【図７】不正なサービスパス提示時の動作を示すシーケンス図である。

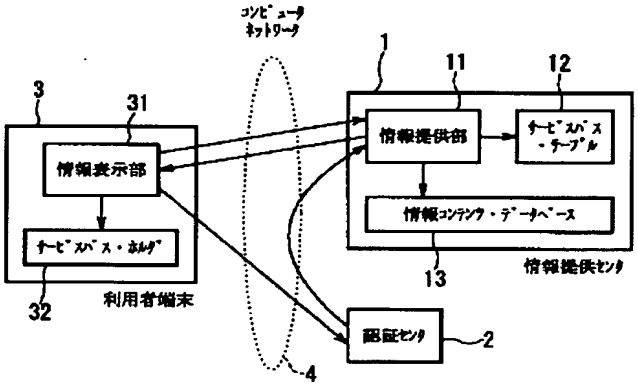
【符号の説明】

１・・・情報提供センタ、
１１・・・情報提供部、
１１ａ・・・WWWサーバ、
１１ｂ・・・情報提供ＣＧＩ部、
１２・・・サービスパス・テーブル、
１３・・・情報コンテンツ・データベース、
２・・・認証センタ、
３・・・利用者端末、
３１・・・情報表示部、
３１ａ・・・WWWブラウザ、
３２・・・サービスパス・ホルダ、
３２ａ・・・クッキー・ファイル、
４・・・コンピュータネットワーク。

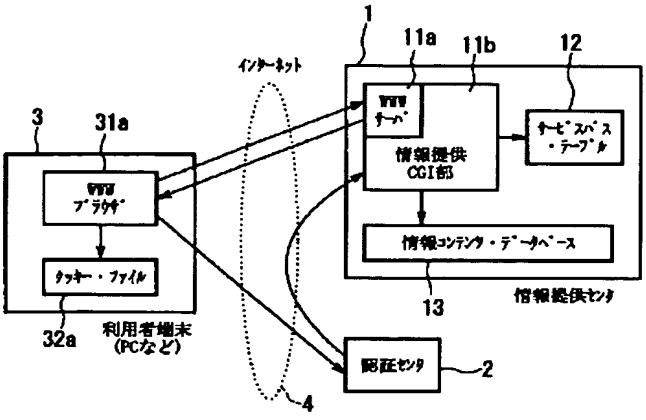
【図１】



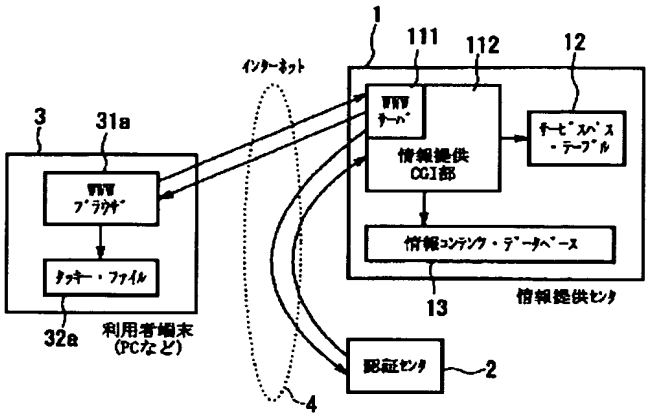
【図２】



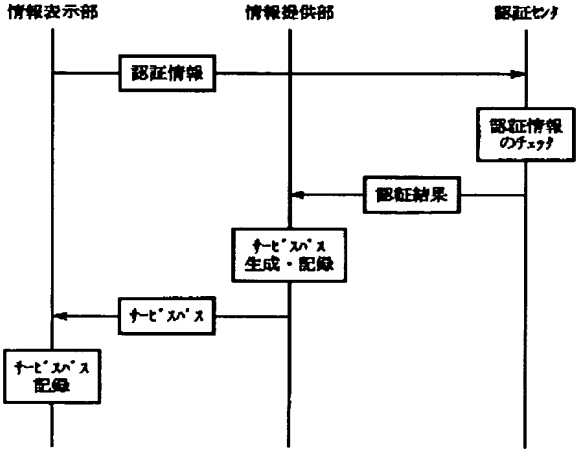
【図３】


1
11a
11b
12
インターネット
3
31a
WWW サーバ
情報提供 CGI部
サービスパス・テーブル
WWW ブラウザ
情報コンテンツ・データベース
クッキー・ファイル
情報提供センタ
13
32a
利用者端末 (PCなど)
認証センタ
2
4

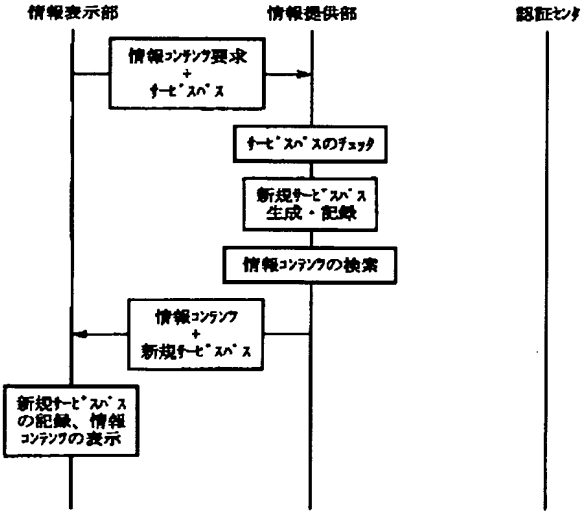
【図４】


1
111
112
12
インターネット
3
31a
WWW サーバ
情報提供 CGI部
サービスパス・テーブル
WWW ブラウザ
情報コンテンツ・データベース
クッキー・ファイル
情報提供センタ
13
32a
利用者端末 (PCなど)
認証センタ
2
4

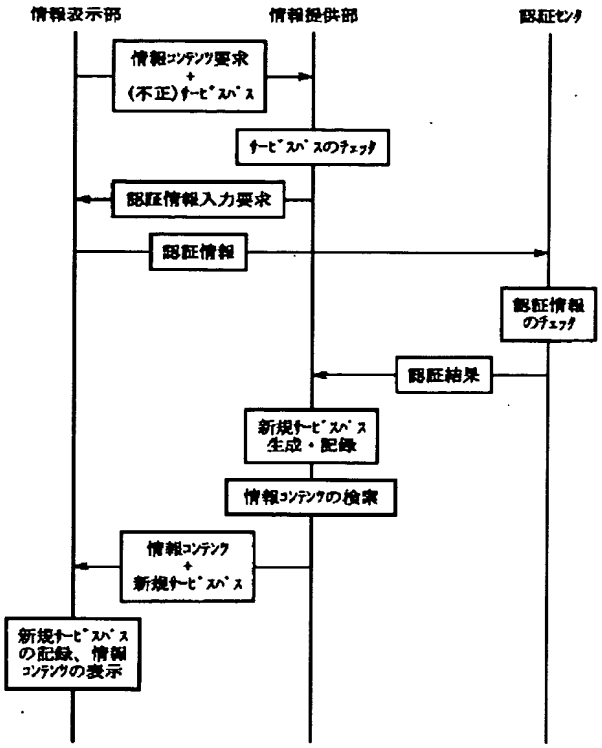
【図５】


情報表示部
情報提供部
認証センタ
認証情報
認証情報のチェック
認証結果
サービスパス生成・記録
サービスパス
サービスパス記録

【図６】


情報表示部
情報提供部
認証センタ
情報コンテンツ要求 + サービスパス
サービスパスのチェック
新規サービスパス生成・記録
情報コンテンツの検索
情報コンテンツ + 新規サービスパス
新規サービスパスの記録、情報コンテンツの表示

【図７】



フロントページの続き

(72)発明者　曽根岡　昭直
東京都新宿区西新宿三丁目19番２号　日本
電信電話株式会社内

Ｆターム(参考)　5B049 AA01 AA05 AA06 BB00 EE23
EE28
5B085 AA08 AE02 AE04 AE23
5B089 GA11 GA21 GB01 GB02 GB09
JA20 JA33 KA03 KA17 KB13
KC15 KC47 KC58 LB14